

UNITED STATES DISTRICT COURT

for the
Eastern District of North Carolina

FILED

FEB 10 2016

JULIE RICHARDS JOHNSTON, CLERK
US DISTRICT COURT, EDNC
BY OR DEP CLK

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 THE PREMISES LOCATED AT 811 S YAUPON
 TERRACE, MOREHEAD CITY, NC 28577

Case No. 4:16-MJ-1022-KS

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A to Affidavit, incorporated herein by reference

located in the Eastern District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B to Affidavit, incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 USC 371	Conspiracy to commit an offense(s) against the United States
18 USC 1030(a)(2)(C)	Fraud and related activity in connection with computers
47 USC 223	Obscene/harrassing telephone calls in DC or in interstate/foreign communications

The application is based on these facts:

See Affidavit of FBI SA BJ Kang, incorporated herein by reference

- ☐ Continued on the attached sheet.
☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

BJ Kang
Applicant's signature

BJ Kang, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 2/10/16

City and state: Greenville, North Carolina

Kimberly A. Swank
Judge's signature

Kimberly A. Swank, United States Magistrate Judge
Printed name and title

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
EASTERN DIVISION**

Case No. 4:16-mj-1022-KS

IN THE MATTER OF THE SEARCH OF
THE PREMISES LOCATED AT 811 S
YAUPON TERRACE, MOREHEAD CITY,
NORTH CAROLINA 28557

UNDER SEAL

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

BJ Kang, a Special Agent with the Federal Bureau of Investigation ("FBI"), being
duly sworn, deposes, and states:

INTRODUCTION AND AGENT BACKGROUND

1. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516, Title 18, United States Code. I make this affidavit in support of an application for a search warrant to search the premises located at 811 S Yaupon Terrace, Morehead City, NC 28557 ("hereinafter the SUBJECT PREMISES"), as further described in Attachment A, because there is probable cause to believe that the SUBJECT PREMISES contain evidence, fruits, and instrumentalities of violations of federal criminal laws having been committed, including 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1030(a)(2)(C) (Fraud and related activity in connection with computers), and 47 U.S.C. § 223 (Obscene or harassing telephone calls in the District of Columbia or in interstate or foreign communications).

2. I have been a Special Agent of the FBI since 2005. During that time I have participated in numerous investigations of fraud relating to the securities markets, including

market manipulation, insider trading, and Ponzi schemes, and I have conducted or participated in arrests, the execution of search warrants, surveillance, debriefings of informants, and reviews of taped conversations and securities trading records. I am currently assigned to the criminal computer intrusion squad of the FBI Washington Field Office (WFO) where I investigate crimes involving computer intrusions. Prior to my assignment to WFO, I was a Supervisory Special Agent at FBI Cyber Headquarters, where I provided support to financially motivated cyber intrusion investigations. I have also received training in cybercrime investigation techniques, computer evidence identification, computer evidence seizure and processing, and analyzing and tracing digital currency.

3. The facts and information contained in this affidavit are based on my personal observations, my training and experience, information obtained from other federal law enforcement officers and witnesses, interviews of victims, review of documents related to this investigation, and information gained through my training and experience. This affidavit only contains such information as is necessary to show there is sufficient probable cause for the requested warrant to search and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts set forth in this affidavit, I submit that there is probable cause to believe that violations of federal criminal laws have been committed, including 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1030(a)(2)(C) (Fraud and related activity in connection with computers), and 47 U.S.C. § 223 (Obscene or harassing telephone calls in the District of Columbia or in interstate or foreign communications), by various individuals, including an individual at the SUBJECT PREMISES. I submit there is also probable cause to search the information described in Attachment A for evidence, fruits, and instrumentalities of violations of these crimes, as further described in Attachment B.

RELEVANT STATUTES

5. *Conspiracy.* 18 U.S.C. § 371 provides, in relevant part, that if two or more persons conspire to commit any offense against the United States, and one or more of such persons do any act to effect the object of the conspiracy, then each shall be guilty of a federal offense.

6. *Fraud and Related Activity in Connection with Computers.* 18 U.S.C. § 1030(a)(2)(C) provides “Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished as provided in subsection (c) of this section.”

7. *Obscene or harassing telephone calls in the District of Columbia or in interstate or foreign communications.* 47 U.S.C. § 223 provides: “Whoever ...in interstate or foreign communications ...makes a telephone call or utilizes a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with intent to abuse, threaten, or harass any specific person...shall be fined under title 18 or imprisoned not more than two years, or both.”

SUMMARY OF PROBABLE CAUSE

8. The FBI is investigating a computer intrusion case in which unknown individual(s) accessed and attempted to access victims' computer accounts without authorization, obtained personal information and posted that information on the Internet for the purpose of harassing the victims. Moreover, the unknown individual(s) then posts derogatory and harassing in nature comments on the Internet about the victims and/or contacts the victims by way of telephone to harass them further. As explained below, there is probable cause to believe that the SUBJECT PREMISES further described below and in Attachment A contains evidence, fruits,

and instrumentalities of unauthorized access and attempted unauthorized access into victims' computer accounts. Records from the SUBJECT PREMISES will help law enforcement determine the volume and scope of unauthorized access activity and identify and locate those responsible.

Reporting and Investigation of Computer Intrusion Activity

9. On or about October 18, 2015, the New York Post published an article entitled "Teen says he hacked CIA director's AOL account." According to the article, an unidentified individual, who described himself as an American high school student, claimed credit for hacking (committing access without authorization into computers) into the AOL account of the Director of the Central Intelligence Agency (CIA). The computer hacker demonstrated to the New York Post reporter that he had control over the Twitter screen name @PHPHAX, also known as Twitter name "Cracka." The computer hacker indicated he was part of a group called "CWA" and explained it stood for "Crackas With Attitude." The computer hacker further indicated CWA refers to him and a classmate. The computer hacker contacted the New York Post to brag about his exploits, which included posting of some of the stolen documents and portion of documents purported to be from the Director of the CIA. The computer hacker claimed the stolen documents were stored as attachments to about 40 emails that he read after breaking into the email account of the Director of the CIA on or about October 12, 2015. The computer hacker indicated he used a technique called "social engineering" which involved tricking workers at Verizon into providing personal information of the Director of the CIA and fooling AOL into resetting the password for his AOL account. The computer hacker subsequently posted to Twitter and other websites several images of documents that he obtained through his access to the AOL account.

10. On or about October 19, 2015, The Hacker News¹ published an article entitled, "High school Student Hacked Into CIA Director's Personal Email Account." The Hacker News article reported that the hacker operated under the Twitter name "Crackas With Attitude," with the Twitter screen name @_CWA_. According to the article, on or about October 19, 2015, @_CWA_ released what it claimed was alleged personal information of 2,611 former and current government intelligence officials on Twitter. The data included phone numbers, Social Security Numbers, email addresses, and security clearance level and employment status in some cases.

11. Subsequent FBI investigation has revealed that @PHPHAX has publicly, via Twitter and via interviews with several news organizations, claimed credit for intruding into personal computer accounts of various individuals, including prominent U.S. Government officials, obtaining personal information and posting that information on the Internet. As described more fully below, FBI investigation has revealed that @PHPHAX has been aided in these attacks by other individuals. Also as described below, the FBI has identified JUSTIN LIVERMAN as a subject of this investigation.

VICTIM 1

12. On or about October 16, 2015, a victim (VICTIM 1) located in the Eastern District of Virginia reported to the FBI that one of VICTIM 1's email accounts was compromised. VICTIM 1 also reported that attempts were made to access VICTIM 1's other online accounts, and that VICTIM 1 had received multiple telephone calls from unknown individual(s) which were harassing in nature. Specifically, VICTIM 1 reported that unknown

¹ The Hacker News is a social news website focusing on computer science and information security.

individual(s) had compromised VICTIM 1's main AOL email account.² VICTIM 1 is a senior U.S. Government official.

13. Subsequent FBI investigation has revealed that several accounts belonging to VICTIM 1 and his/her family members were compromised by @PHPHAX.

VICTIM 2

14. On or about November 1, 2015, a victim (VICTIM 2) located in Georgia reported to the FBI that he/she had received multiple telephone calls on VICTIM 2's home telephone line from an unknown individual or individual(s) which were harassing in nature. VICTIM 2 is a senior U.S. Government official who works for a federal law enforcement agency.

15. Subsequent FBI investigation has revealed that the Comcast Internet Service Provider (ISP) account belonging to VICTIM 2 and his family was compromised by @PHPHAX as well as possibly his co-conspirators.

VICTIM 3

16. On or about December 19, 2015, a victim (VICTIM 3) located in the Eastern District of Virginia reported to the FBI that VICTIM 3 had received information from Comcast, their ISP, that their Comcast account password was changed on or about December 19, 2015. VICTIM 3 also reported that he/she received a telephone call that was harassing in nature from an unknown individual. VICTIM 3 is a senior U.S. Government official who works for a federal law enforcement agency.

² According to AOL, Inc.'s website, the username you create when you first register for an AOL account is considered the primary master username. The primary master username has the power to designate up to six general usernames as designated master usernames. The primary master username will always have the master username status (this name can't be changed). All master usernames can change the account's billing method and price plan; change passwords for other usernames on the account; create, delete, and restore any username on the account, except the primary master username and other functions.

17. Subsequent FBI investigation has revealed that the Comcast ISP account belonging to VICTIM 3 was compromised on or about December 19, 2015.

VICTIM 4

18. On or about December 26, 2015, the FBI discovered via review of social media that the Verizon account belonging to a senior White House employee (VICTIM 4), who resides in the Eastern District of Virginia, had been compromised. Specifically, on or about December 12, 2015, @BASHTIEN_ announced via public Twitter posts that he and two other Twitter users (Cracka and @_D3F4ULT) had compromised VICTIM 4's Verizon account.

19. Subsequent FBI investigation has revealed that the Verizon account belonging to VICTIM 4 and his/her family was compromised by @PHPHAX as well as possibly his co-conspirators.

VICTIM 5

20. On or about November 30, 2015, the FBI discovered via review of social media that @PHPHAX posted a series of tweets suggesting that he had hacked an email account belonging to the U.S.-based CEO of a financial services holding company (VICTIM 5). @PHPHAX also tweeted photographs purported to be of VICTIM 5 and his/her family members.

21. Subsequent FBI investigation revealed that the mobile device that contained VICTIM 5's private family photographs may have been compromised by @PHPHAX as well as possibly his co-conspirators.

VICTIM 6

22. On or about December 28, 2015, the FBI discovered via review of social media that accounts belonging to an individual (VICTIM 6) and his/her spouse had been compromised.

VICTIM 6 is CEO of a company that provides critical services such as intelligence, cyber, and IT to government and private sector customers. Specifically, on or about December 28, 2015, @DICKREJECT announced via Twitter that he had compromised VICTIM 6's LinkedIn³ account as well as the Facebook account belonging to VICTIM 6's spouse.

Twitter Handle @PHPHAX

23. On or about October 27, 2015, Twitter was served with a search and seizure warrant issued by a Magistrate Judge sitting at the United States District Court for the Eastern District of Virginia for records associated with several Twitter accounts, including @PHPHAX. Some of the information described below is taken from the FBI's review of information obtained through that search and seizure warrant.

24. On or about November 1, 2015, at approximately 4:18 pm, EST, @PHPHAX publicly posted the following on Twitter: "welp, I sense another gov official's email contact list drop." Less than an hour later, @PHPHAX publicly posted on Twitter, "anddddddd here we go again imfao IF YOU OWN A AOL ACCOUNT YOU CAN JOIN THE GOVERNMENT RIGHT NOW!!" This Twitter post was accompanied by what appears to be a screenshot showing VICTIM 2's name and his redacted U.S. Government-issued email addresses.

25. A review of Twitter account records for @PHPHAX showed that on or about November 2, 2015, at approximately 12:19:56am, EST, @PHPHAX publicly tweeted what appears to be a screenshot of VICTIM 2's Comcast Xfinity monthly bill that is partially redacted.

Twitter Handle @DICKREJECT

26. On or about December 12, 2015, Twitter suspended the account of Twitter handle @PHPHAX, also known as "Cracka."

³ LinkedIn is a business-oriented social networking service.

27. On or about December 23, 2015, Twitter name "Cracka" aka @DICKREJECT, publicly tweeted, "ok you told me to make a twitter now wtf do i do." The next day, @DICKREJECT publicly tweeted, "watch me become bigger than @kevinmitnick."⁴

28. On or about December 24, 2015, at approximately 5:39 pm, EST, @DICKREJECT publicly tweeted, "hello @FBI." This tweet was accompanied by what appears to be a screenshot of an FBI database web page with the words, "Signed onto Criminal Justice Information Services Division as [VICTIM 2's government issued email addresses]."

29. On or about December 24, 2015, at approximately 5:59 pm, EST, @DICKREJECT publicly tweeted, "Merry Christmas @FBI [VICTIM 3] Call Logs cryptobin.org/a3q7g9r7⁵ Password is lol." This Cryptobin link contained several pages worth of VICTIM 3's call records from on or about September 20, 2015 to on or about December 16, 2015.

30. On or about December 24, 2015, at approximately 6:04 pm, EST, @_D3F4ULT publicly tweeted, "these [derogatory term] aint ready for the carnage #CWA." This tweet was accompanied by a screen shot of a character from the movie Batman and the words, "AND HERE..WE...GO."

31. On or about December 24, 2015, at approximately 6:39 pm, EST, @DICKREJECT publicly tweeted, "ohhhhh so much unpublished data." This tweet included a redacted screenshot of an individual's name and his/her purported affiliation with the National

⁴ Twitter handle @kevinmitnick is the Twitter handle for Kevin Mitnick. Mitnick is best known in the hacking community for his high-profile 1995 arrest and subsequent conviction for various computer-related crimes in which he utilized social engineering techniques.

⁵ Cryptobin, similar to Pastebin, is a popular website for storing and sharing text. Though Cryptobin and Pastebin are used for distributing legitimate data, it seems to be frequently used as a public repository of stolen information.

Security Agency (NSA). A few minutes later, at approximately 6:43 pm, EST, @DICKREJECT publicly tweeted, "nice @Secret Service." This tweet included a redacted screenshot of an individual's name and his/her purported affiliation with the United States Secret Service (USSS). Twitter handle @DICKREJECT's public release of these two redacted screenshots of government employee names and their respective agencies is consistent with the way @PHPHAX released such information before @PHPHAX was suspended by Twitter.⁶

32. On or about December 27, 2015, at approximately 8:07 am, EST, @DICKREJECT publicly tweeted, "Merry Christmas to [VICTIM 5]." This tweet included a photograph of VICTIM 5 and another family member. Approximately six minutes later, @DICKREJECT publicly tweeted another photograph of VICTIM 5 with other family members.

33. Later that same day (on or about December 27, 2015), @_D3F4ULT and @BASHTIEN_ each re-tweeted @DICKREJECT's posts that contained the above-described family pictures belonging to VICTIM 5.

34. On or about December 27, 2015, at approximately 4:09 pm, EST, @DICKREJECT publicly tweeted, "There seems to be some strange posts coming from [VICTIM 6] wife's facebook account." This tweet included a partial screenshot of VICTIM 6's purported Facebook messages. For example, one of VICTIM 6's purported Facebook messages states, "The US government funds Israel so they can kill innocent people in Palestine. The US government and the Israel government are the real terrorists. Bush Did 911. Jet fuel doesn't melt steel beams."

⁶ For example, on or about November 4, 2015, @PHPHAX, using VICTIM 2's computer credentials he had obtained via social engineering, gained unauthorized access in to portions of the Law Enforcement Enterprise Portal (LEEP). LEEP is a gateway providing law enforcement agencies, intelligence groups, and criminal justice entities access to resources such as Joint Automated Booking System (JABS). On or about November 5, 2015, @PHPHAX publicly posted, "Can the gov hear me now? Will they help free Palestine now?" This post included a screenshot of three partially redacted names and their respective official government email addresses, title, and organization.

35. On or about December 27, 2015, at approximately 4:13 pm, EST, @_D3F4ULT re-tweeted @DICKREJECT's tweet about VICTIM 6's Facebook account. Moreover, at approximately 4:23 pm, EST, @_D3F4ULT publicly tweeted, "oh not much, just chillen, eating watermelon and watching my ninja @dickreject destroy [VICTIM 6's company] #CWA." That same day, @BASHTIEN_ also re-tweeted @DICKREJECT's tweet about VICTIM 6's Facebook account.

36. On or about December 28, 2015, at approximately 5:23 am, EST, @DICKREJECT publicly tweeted, "this ceo is a fucking retard hahahha." Less than twenty minutes later, @DICKREJECT publicly tweeted, "whats happened to [VICTIM 6's name] LinkedIn? Linkedin.com/[VICTIM 6's name]." This tweet included a screenshot of VICTIM 6's defaced LinkedIn page that included, "recently fucking rekt⁷ by cracka."

37. Later that same day (on or about December 28, 2015), @_D3F4ULT re-tweeted @DICKREJECT's tweet about VICTIM 6's defaced LinkedIn page.

38. On or about December 28, 2015, at approximately 6:49 am, EST, @DICKREJECT publicly tweeted, "hahahhah." This tweet included what appears to be a screenshot of VICTIM 6's wife's Facebook page with a message to others about her Facebook account. The message read, "I have been hacked with nasty comments, please ignore them."

39. On or about December 28, 2015, at approximately 8:04 pm, EST, @_D3F4ULT made the following post: "shouts to [VICTIM 6's wife] for showing #AnonSec⁸ that love &

⁷ "Rekt" is an Internet slang term for "wrecked" that is often used in online gaming to indicate that someone has been defeated or embarrassed.

⁸ AnonSec is a hacking collective affiliated with Anonymous that claims to have hacked over 700 websites. As described below, @_D3F4ULT claims on his Twitter page to be "A Official Admin of #AnonSec."

becoming a whistleblower[.]” This tweet included a screenshot that appears to show VICTIM 6’s wife’s compromised Facebook page.

40. On or about December 28, 2015, at approximately 8:20 pm, EST, @DICKREJECT tweeted a hashtag for FreePalestine. This tweet included what appears to be a screenshot of VICTIM 6’s wife’s defaced Facebook message response to one her friend’s messages that read, “If you are a friend of [VICTIM 6’s wife], please be aware that her account has been hacked and ignore any offensive posts. They are not from [VICTIM 6’s wife].” The purported response from VICTIM 6’s wife reads: “BITCH HOW IS SAYING FREE PALESTINE OFFENSIVE?! STUPID FUCK FREE PALESTINE FUCK ISRAEL FREE PALESTINE FUCK ISRAEL.”

Twitter Handle @_D3F4ULT

41. @_D3F4ULT’s Twitter persona on his Twitter page profile bio states that he is “A Official Admin of #AnonSec...All your drones are belong to us.” The name “Default Virusa” is tied to Twitter handle @_D3F4ULT. Twitter handle @SH1N0D4 is listed in @_D3F4ULT’s Twitter page profile bio.

42. FBI’s review of @PHPHAX’s Direct Messages⁹ (DMs) obtained pursuant to the above-described October 27, 2015 search and seizure warrant included several DMs between @PHPHAX and @_D3F4ULT. For example, in one exchange that occurred on or about October 20, 2015 between approximately 10:15 pm and 10:39 pm, EDT, @_D3F4ULT congratulated @PHPHAX on his recent compromise of accounts belonging to individuals

⁹ DMs let you send your contacts private notes through Twitter. Unlike regular tweets, the only person who can see a DM is the recipient.

associated with the CIA and Department of Homeland Security. @_D3F4ULT also advised @PHPHAX to “stay safe and dban¹⁰ any drive dont need bro.”

43. On or about November 2, 2015, at approximately 12:19 am, EST, @_D3F4ULT publicly tweeted, “When you're [VICTIM 2] but your wife still pays for the internet @phphax,” along with a screenshot, showing what appears to be a redacted version of a Comcast Xfinity payment dated September 7, 2015 for VICTIM 2’s Comcast account. As described above in paragraph 25, @PHPHAX tweeted the same screenshot of VICTIM 2’s Comcast Xfinity bill at approximately the same date and time (November 2, 2015, at approximately 12:19:56 am, EST) as @_D3F4ULT’s public tweet just described.

Twitter Handle @BASHTIEN

44. On or about December 12, 2015, at approximately 4:56 pm, EST, @BASHTIEN_ publicly tweeted, “dis is @Snowden, I heard u talkin shit [Twitter handle associated to VICTIM 4] so i tok ur acc bish!” The post included a defaced image of a Verizon account’s sign-in page that included reference to three Twitter users, “cracka_d3f4ult_bashtien_2015” below the Verizon site key image of a snow man.

45. Based on FBI’s review of audio recordings and log files obtained from Verizon pursuant to legal process, an individual who is believed to be the user of Twitter handle @DICKREJECT (previous Twitter handle of @PHPHAX) contacted Verizon call centers on multiple occasions beginning on or about December 10, 2015 to attempt to gain access into VICTIM 4’s Verizon account. Logs maintained by Verizon for VICTIM 3’s account show that on two occasions on or about December 12, 2015 (at approximately 11:21 am and 11:26am, EST), VICTIM 4’s Verizon site key image was modified. The IP addresses that accessed

¹⁰ Darik’s Boot and Nuke (DBAN) is a free data wipe program to permanently erase all the files from a computer hard drive.

VICTIM 3's Verizon account to modify the site key image are associated to anonymous IP addresses.

46. Based on my training and experience, I believe that the inclusion of those names under the Verizon site key image of a snow man indicates a claim of responsibility by those responsible for the account's compromise. As described above, @PHPHAX goes by the name "Cracka." Moreover, later in the day on or about December 12, 2015, @_D3F4ULT re-tweeted the original post (described in paragraph 44) tweeted by @BASHTIEN_.

47. On December 26, 2015, at approximately 5:51 pm, EST, @DICKREJECT publicly tweeted, "@fur_f4g3t go to verizon.com and put in her username [VICTIM 4], its still there @Bashtien_ @Snowden [VICTIM 4's Twitter handle] @_d3f4ult." One minute later, @DICKREJECT publicly tweeted the same defaced image of the Verizon account's sign-in page as described in paragraph 44.

Twitter Handle @SH1N0D4

48. On or about January 8, 2016, at approximately 12:29 pm, EST, @SH1N0D4 made the following Twitter post in which he appears to give credit for the compromise of the Facebook account belonging to VICTIM 6's wife to @_D3F4ULT: "[Victim Company]'s CEOs wife caught by @_D3F4ULT supporting terrorist Junaid Hussain(TriCk)¹¹ & admitting incest." The post was accompanied by a picture of an apparent December 27, 2015 conversation on Facebook in which the hacked spouse's Facebook account engages in a lurid "conversation" with Facebook user "Joseph Markowicz" that occurred between 4:01 p.m. and 4:04 p.m. The FBI's investigation into "Joseph Markowicz" is described more fully below.

¹¹ Junaid Hussain was a British hacker who had joined ISIS and is reported to have been killed in an air strike.

49. On January 8, 2016, at approximately 12:49 pm, EST, @_D3F4ULT re-tweeted @SH1N0D4's tweet and the screenshot of the lurid "conversation" described above.

Facebook aliases Joseph Markowicz and Blastphamous

50. In response to legal process, in or about November 19, 2015, Twitter provided records for Twitter handle @_D3F4ULT. The information provided by Twitter included IP address log-in history for an approximately two-month period in late 2015, specifically from on or about September 21, 2015 to on or about November 3, 2015. One of the IP addresses used to access the Twitter handle @_D3F4ULT Twitter account during that period (on or about October 31, 2015) was IP address 65.184.190.234, which is provided by Time Warner Cable. According to information provided by Twitter, on or about November 1, 2015, @BASHTIEN_ used the same IP address (65.184.190.234) to access his account as @_D3F4ULT used only the day before (on or about October 31, 2015). For these reasons, the FBI believes that Twitter accounts @_D3F4ULT and @BASHTIEN_ may be shared by one or more users.

51. Time Warner Cable provided information to the FBI in response to legal process that IP address 65.184.190.234 was subscribed to, at the time of the access to the @_D3F4ULT and @BASHTIEN_ Twitter accounts, by a woman named Edith Liverman located at "811 S Yaupon Ter, Morehead City, NC." The FBI believes based on open source checks that this address corresponds to "811 S Yaupon Terrace, Morehead City, North Carolina 28557," i.e., the SUBJECT PREMISES.

52. On or about January 5, 2016, the FBI conducted open source research into Edith Liverman and her address. These checks revealed that JUSTIN LIVERMAN, a 23 year-old male also resides at this address. A review of JUSTIN LIVERMAN's Facebook page revealed that he is heavily involved in computer information technology and includes multiple mentions of the

hactivist collective known as Anonymous. On his Facebook and LinkedIn pages, JUSTIN LIVERMAN lists himself as a "Security Research" at Bugcrowd, Inc. and HackerOne, and since March 2015, as a "Journalist" at cyberwarezone.com.¹²

53. In January 2016, the FBI conducted several law enforcement database (Accurant) queries for the SUBJECT PREMISES. According to this law enforcement database, Justin G Liverman, a 23 year-old male, is an occupant of the SUBJECT PREMISES. Moreover, the Accurant report lists a Verizon Wireless cellular telephone number of (252) 808-5854 as being associated to JUSTIN LIVERMAN. According to this same information, Coastal Heating & Cooling, Inc., is also associated with the same address (811 S Yaupon Terrace, Morehead City, North Carolina). On his LinkedIn page, JUSTIN LIVERMAN states that he was a Technician for Coastal Heating and Cooling, Inc., for approximately four years.

54. FBI investigation has revealed that the user of @_D3F4ULT may use the alias of "Joseph Markowicz." FBI's review of Twitter records in response to legal process shows that email address "D3F4ULT@Protonmail.ch" was included in @_D3F4ULT's Twitter account. In late December 2015, a U.S.-based Bitcoin exchange advised that their records showed that the email address "D3F4ULT@Protonmail.ch" was used to create an account that is registered to "Joseph Markowicz." Moreover, the Joseph Markowicz Facebook account has the same user display image as the @_D3F4ULT Twitter page and the user provided intro for his Facebook

¹² Cyberwarzone.com is a website that purports to provide "reliable cybercrime and cyberwar news." Cyberwarzone.com states on its website that it is a Netherlands-based company that was founded in January 2010 by an entrepreneur named Reza Rafati. The FBI has been unable to determine if Cyberwarzone.com employs any paid staff. A review of their website reveals that the website posts approximately one article/post a day. On the "About Us" section of the website, under the heading "What we are always searching for," Cyberwarzone.com states that it is always looking for contributors, stating as follows:

Cyberwarzone.com is always searching for people that are interested in leaving their knowledge on the website – if you have the time to post cyber resources like Youtube videos, Hacktivism operations, cyber conflict, espionage or hacking news and you have want to help us out then we would appreciate it a lot!

account states, "Data Pirate at Anonsec Hackers." In addition, the information contained on the Joseph Markowicz Facebook page is almost identical in content to that contained on the @_D3F4ULT Twitter page.

55. In response to legal process, on or about January 13, 2016, Facebook provided records for the "Joseph Markowicz" Facebook account. The records provided by Facebook showed that the user used the same email address that was used to sign up for the Twitter handle @_D3F4ULT, specifically "D3F4ULT@Protonmail.ch. Moreover, the majority of the accesses to the Joseph Markowicz Facebook account for the period of on or about August 16, 2015 to or on about December 30, 2015, were from the same proxy IP address that was used almost exclusively to access @_D3F4ULT's Twitter account for the time period of on or about September 21, 2015 to on or about November 3, 2015.

56. In January 2016, the FBI queried the open source Spokeo¹³ database for the name JUSTIN LIVERMAN at the SUBJECT PREMISES. The records provided by Spokeo listed a Facebook account "BlastPhamous" as being associated with JUSTIN LIVERMAN.

57. In response to legal process, on or about February 1, 2016, Facebook provided records for the "BlastPhamous" Facebook account. The records provided by Facebook revealed that the majority of the IP addresses used to access the BlastPhamous Facebook account for the period of on or about March 22, 2015 to on or about November 17, 2015 were IP addresses provided by Time Warner Cable. Moreover, on or about July 22, 2015 and on or about August 15, 2015, the BlastPhamous Facebook account was accessed by IP address 65.184.190.234. As described above in paragraph 51, this Time Warner IP address was subscribed to by Edith

¹³ Spokeo is a people search website that aggregates data from online and offline sources.

Liverman located at the SUBJECT PREMISES. Records checks show that Edith Liverman is 86 years-old and is believed to be JUSTIN LIVERMAN's grandmother.

Alleged Breach of National Aeronautics and Space Administration (NASA) Database and Twitter Handle @OPNASADRONES

58. On or about January 28, 2016, at approximately 7:36 pm, EST, @OPNASADRONES publicly tweeted, with the text upside down and backwards, "All your drones are belong to AnonSec @NASA." As described in paragraph 41, this quote about drones is the same quote used by @_D3F4ULT in his Twitter page profile bio.

59. On or about January 29, 2016, at approximately 8:45 am, EST, @_D3F4ULT publicly tweeted, "Go follow @OpNasaDrones for the new leaks coming [smiley face] #AnonSec."

60. On or about January 30, 2016, at approximately 12:43 pm, EST, @OPNASADRONES publicly tweeted, "T-Minus 24hrs until #OpNasaDrones leaks & zine released...#AnonSec." @_D3F4ULT re-tweeted this post approximately 11 minutes later.

61. On or about January 31, 2016, at approximately 9:50 am, EST, another user (@An0nKn0wledge) publicly tweeted, "@_d3f4ult so whens the leak today? Im Eagerly waiting to see what u guys have for us ;) #OpNasaDrones I hope ur claims hold true. ;D."

62. On or about January 31, 2016, at approximately 12:01 pm, EST, @_D3F4ULT re-tweeted, "@Sh1n0d4 #OpNasaDrones." This re-tweet was accompanied by a screen shot of a character from the movie Batman and the words, "AND HERE..WE...GO." Approximately four minutes later, @OPNASADRONES publicly tweeted, "[+] #OpNasaDrones Zine by #AnonSec [+] pastebin.com/Ws67FPBr cryptobin.org/b2b572s9 passwd: anonsec." Review of the pastebin and cryptobin pastes revealed that the information contained in each paste appeared to be similar. The paste purports to contain approximately 2,400 names, email addresses, and

telephone numbers of NASA employees. The paste also contains other data that is alleged to be sensitive NASA data, including video footage obtained from drones allegedly operated by NASA. The paste also purports to include chat sessions among several members of #AnonSec, including @SH1N0D4, @BASHTIEN_, and @_D3F4ULT, in which the members discuss the sensitive NASA data.

63. Later that same day (January 31, 2016), Infowars.com, an online news group, published an article titled, "Hackers Allegedly HiJack Drone After Massive Breach at NASA. Hackers release 631 aircraft and radar videos, 2,143 flight logs and data on 2,414 employees." The article states that the author obtained the collection of files from AnonSec admin "Default Virusa." As described in paragraph 41, "Default Virusa" is the name associated with @_D3F4ULT's Twitter handle.

64. In January 2016, the FBI obtained driver's license information for LIVERMAN. LIVERMAN's North Carolina Driver's License lists his full name as JUSTIN GRAY LIVERMAN with the address of 811 S Yaupon Terrace, Morehead City, North Carolina 28557, the SUBJECT PREMISES.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

65. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

66. *Probable cause.* I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

67. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT REMISES because:

a. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, and internet history) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contains information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media

access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

b. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a

computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

e. I know that when an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

68. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded

on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

e. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

f. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

g. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

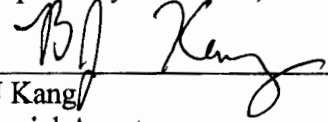
h. Because several people may share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are

predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

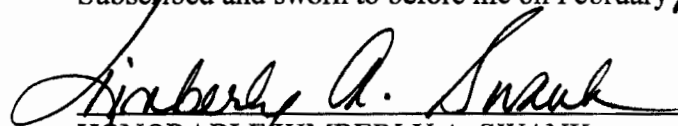
69. Based on the aforementioned information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations, or attempted violations of Title 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1030(a)(2)(C) (Fraud and related activity in connection with computers), and 47 U.S.C. § 223 (Obscene or harassing telephone calls in the District of Columbia or in interstate or foreign communications) may be located at SUBJECT PREMISES, as further described in Attachment A. I request that the Court issue the proposed search warrant for the SUBJECT PREMISES to search for items described in Attachment B.

Respectfully submitted,



BJ Kang
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on February 10 2016



HONORABLE KIMBERLY A. SWANK
United States Magistrate Judge

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
EASTERN DIVISION**

Case No. _____

IN THE MATTER OF THE SEARCH OF
THE PREMISES LOCATED AT 811 S
YAUPON TERRACE, MOREHEAD CITY,
NORTH CAROLINA 28557

UNDER SEAL

ATTACHMENT A

Property to Be Searched

The SUBJECT PREMISES is known and described as 811 S Yaupon Terrace, Morehead City, North Carolina 28557. The SUBJECT PREMISES is a single story, single-family ranch style brick house with a red door. While facing the front of the SUBJECT PREMISES, the driveway is on the right hand side of the house. Aerial view shows a detached building behind the back of the SUBJECT PREMISES.

The premises to be searched include any appurtenances to the real property that is the SUBJECT PREMISES of 811 S Yaupon Terrace, Morehead City, North Carolina 28557 and any storage units/outbuildings. Due to the ability and ease for individuals to store evidence of the crimes under investigation onto media storage devices such as CDs, DVDs, and thumb drives (further described in Attachment B), which can be easily concealed and stored inside of a vehicle, the premises to be searched includes vehicles owned by the occupants of the SUBJECT PREMISES.





**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
EASTERN DIVISION**

Case No. _____

IN THE MATTER OF THE SEARCH OF
THE PREMISES LOCATED AT 811 S
YAUPON TERRACE, MOREHEAD CITY,
NORTH CAROLINA 28557

Case No. 1:16-sw-____

UNDER SEAL

**ATTACHMENT B
Items To Be Seized**

The following items to be seized are evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1030(a)(2)(C) (Fraud and related activity in connection with computers), and 47 U.S.C. § 223 (Obscene or harassing telephone calls in the District of Columbia or in interstate or foreign communications):

- (1) Computers or storage media used as a means to commit the violations described above;
- (2) For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crimes under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crimes under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- m. contextual information necessary to understand the evidence described in this attachment.

(3) Routers, modems, and network equipment used to connect computers to the Internet;

and

(4) Records, information, and items relating to violations of the statutes described above,

including, but not limited to:

- a. Records, information, and items relating to the occupancy of the SUBJECT PREMISES including utility and telephone bills, mail envelopes, or addressed correspondence;

- b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes; and
- c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.